Network Design Strategies

CHAPTER 3

SOME OF THE MAIN TOPICS IN THIS CHAPTER ARE

Many types of networks were discussed in Chapter 1, "A Short History of Computer Networking," from ARPANET to TCP/IP. And in Chapter 2, "Overview of Network Topologies," you learned about the various topologies you can employ when designing and creating a local area network (LAN), and we also looked at some scenarios in which several networks were connected to form a wide area network (WAN). In this chapter, we will look at another aspect of creating a network: the network's logical and physical design. The physical aspects of your LAN will depend on the underlying physical transport technology—Ethernet or Token-Ring, for example, or possibly ATM, which is supported as a LAN protocol in products such as Windows 2000/XP, Windows Server 2003, and Linux. Depending on which technology you use, there will be one or more LAN topologies from which to choose.

Note

Although there are other LAN technologies, such as ARCnet and Novell's IPX/SPX, these are basically legacy products that are no longer being deployed in newer networks. For example, ARCnet is now used mostly in vertical-market applications (such as on the factory floor, or for point-of-sale cash registers). If you don't need the features that TCP/IP provides, and don't need an Internet connection, then these older protocols may be a workable solution for your network. Novell's NetWare products, while allowing for backward compatibility with the IPX/SPX protocol, have finally caught up with the times, and new installations will more than likely use the IP protocol. Other protocols, such as Microsoft's LAN Manager and NetBEUI, are used only in older networks. If you are still using older proprietary protocols, you should consider upgrading to TCP/IP, which is now the de facto standard, from the worldwide Internet down to the LAN.

Before you can begin to design a physical network, however, you first must determine your needs. What services must you provide to your user community? What are the resources you'll need? If you have to compromise, what will it take to satisfy the most users or to provide the more important services? You then will have to take into account network protocols, applications, network speed, and, most important, network security issues; each of these figures into a network's logical design. Another important factor your management will probably force you to consider is cost—you can't forget the budget. These factors make up the logical design for your network. You first should decide what you need and what it will take to provide for those needs.

If you are creating a new network and purchasing new applications, you will probably spend most of your time considering the licensing and other financial costs (training users, network personnel, and so on). If you are upgrading older applications, several other factors come into consideration. Many applications that were coded using COBOL, BASIC, FORTRAN, and other languages that helped jumpstart the computer age may have built-in network functionality based on older proprietary network protocols. If this is the case with your network, you have to consider several things. What will it cost to update thousands of lines of code (or more) to more modern versions of the same programming language? What will it cost to upgrade these programs to newer object-oriented languages? To save money, can you upgrade part of your network and use gateway hardware/software to connect to older network components?

Because of the costs associated with coding applications that were created many years ago, and the expenses that will be required to update them to modern programming languages, you may be forced to maintain legacy applications for a few years while replacement applications are designed and created. You may find a packaged application that can be used to replace older programs. This problem will apply mostly to proprietary computer architectures, instead of Windows or Unix platforms. If you can simply make minor changes and compile the source code so that it will run on a newer operating system, your costs will be much less than if you have to re-create the applications your users need from scratch. Another cost associated with upgrading to new programs is training users and help-desk personnel.

Planning a Logical Network Design

When you plan a logical network design, you can start from one of two places. You can design and install a new network from scratch, or you can upgrade an existing network. Either way, you should gather information about several important factors before you begin the logical design. For example, depending on the services that will be provided to clients, you might need to analyze the possible traffic patterns that might result from your plan. Locate potential bottlenecks and, where possible, alleviate them by providing multiple paths to resources or by putting up servers that provide replicas of important data so that load balancing can be provided. The following are other factors to consider:

- Who are the clients? What are their actual needs? How have you determined these needs—from user complaints or from help-desk statistics? Is this data reliable?
- What kinds of services will you provide on the network? Are they limited in scope? Will any involve configuring a firewall between LANs? And if so, that still doesn't account for configuring a firewall to enable access to the Internet.
- Will you need to allow an Internet connection for just your internal network's users, or will use you need to allow outside vendors access to your network? One example that comes to mind is the Internet Printing Protocol (see Chapter 24, "Overview of the TCP/IP Protocol Suite"). What will it cost to evaluate what kind of services user groups need to access from the Internet? Will you need to allow all users to use email—both within the internal network and through the firewall on the Internet? The same goes for what sites users will be allowed to access using a network browser and other network applications. Will you have users who work from home and require dial-in or VPN access through the Internet?

Note

A hot topic in many companies revolves around just how important it is to let all users have unlimited access to the Internet. If users need to exchange email with vendors, outside consultants, or customers, for example, then you should be sure to send this traffic through a content filter or firewall, and use virus-protection software to detect and prevent malicious code or virus-infected attachments.

Applications such as FTP allow users to send or receive files from remote systems. Can you trust each employee to use this application without abusing it? From a security point of view, it is usually considered very improper to allow any new application to be loaded on any computer—desktop or server—without first submitting the application to testing to ensure that is necessary and is not a security risk. Don't leave any backdoors into or out of your network. More information about securing your network can be found in Chapter 44, "Security Issues for Wide Area Networks," and Chapter 45, "Firewalls."

- Can your users tolerate a little downtime now and then due to network problems, or is it necessary to provide a high-availability network? Will you need clustered servers to provide for a high degree of uptime, or do your users' applications not suffer from a temporary loss of the use of a server? To provide for maximum uptime, can you afford to build redundancy into your network? For example, Chapter 2 discusses redundant topologies that can be used to prevent a single point of failure from making the network (and its resources) unavailable. Chapter 11, "Network Attached Storage and Storage Area Networks," describes methods you can use to mirror data at geographically distant locations.
- In an existing network, will you keep the current protocol or upgrade to a different protocol standard? If you create a network from scratch, what factors should affect your network protocol decision? Ethernet is the most popular LAN technology in the world today. TCP/IP is the most popular protocol suite that runs on Ethernet. Yet there are cases in which other technologies have their niches. Consider the implications (such as support costs and security) to maintain older, proprietary protocols.

Who Are Your Clients?

This seems like a very simple question. However, I'm not saying, "What are your clients' names and how well do you know their children?" I am referring instead to your knowledge of the job descriptions for the users on the network. You need to assess work patterns for various departments so that you can appropriately place servers, high-bandwidth links, and other such things in the appropriate physical location of the network. If most of the network traffic you expect to see will come from the engineering department, you'll need to provide that department with a large data pipe. In Chapter 4, "Upgrading Strategies and Project Management," you'll find more information about surveying the user community to come up with a plan that places resources where they are needed.

What Kinds of Services or Applications Will the Network Offer?

Of course, everyone knows that the most important function of a network today is to support multiuser gaming. Seriously, though, you need to make a list of the kinds of applications currently in use, as well as a list of those requested by users. Each application should have a written risk assessment document that points out potential security problems, if any. Typical network applications today include FTP, telnet, and, of course, browsing the Web. There are "secure" versions of these applications and there are versions that leave a door wide open into your network. Whatever list of applications you chose to support over the network, keep in mind two things:

- Is the application safe? Most applications today come in secure versions or can be used with a proxy server to help minimize the possibility of abuse. Yet, as we all have seen, even the largest corporations are targets at times, and those companies have the staff that should be able to prevent these things from happening. Because proxy servers are an important component of firewalls, this subject is covered in greater detail in Chapter 45. If you want a secure network, this is highly recommended reading!
- Does one application overlap another? Every user has his or her favorite application. Some people like one word processor, whereas others prefer a different one. But when dealing with applications or application suites (such as Microsoft Office), you'll find it better to make a decision and stick with a single product if it can satisfy the needs of your users. They might not like it, and training might be necessary, but supporting multiple applications that do the same thing wastes money and leads to confusion.

A commonly overlooked method for getting data files out of a network and onto the Internet is to simply send the files as an attachment to an email. So if you think you've blocked file transfers by disabling FTP access through the firewall, this example should show that you really do need to do a thorough evaluation of any new application or service you will allow on the network. New applications should be justified with facts that show why they are needed. If an existing application can be used to accomplish the same goal, why do you need another application? Should you retire the older application and use a newer one? Pay attention to the details. And don't forget to test new applications to ensure that they perform as expected. The same goes for older applications—will they work on the new or upgraded network?

Lastly, do you monitor network usage? Do you want to permit users to spend their days browsing the Net, or checking personal email while at work? Many companies have policies that apply to using the telephone for personal business. Do you overlook this situation when giving users email capability? Are you preventing access to sites that are obviously not business-related?

What Degree of Reliability Do I Require for Each Network Link?

Just how much downtime is acceptable? For most users, the answer would be zero. Important components of your network, such as file servers, should have fault tolerance built in from the bottom up. In large servers, you'll find dual-redundant power supplies (each connected to a separate UPS), and disk arrays set up using RAID techniques to provide for data integrity in the event that a disk goes south. If a link between two offices needs to be up 100% of the time, you should plan for multiple links between the two sites to provide a backup capability. In this case, you also can justify the cost of the extra link by using load balancing so that network response time is improved. And, if you are using multiple links to remote sites, it's always a good idea to have more than a single path to the site. At one site this author worked at, there were redundant power lines bringing electricity into the site—side-by-side. If a tree falls, will it bring down one or both of those power lines?

Note

In addition to dedicated links between sites, the use of Virtual Private Networking (VPNs) is becoming a popular method for connecting to remote sites. The advantages of using a VPN are that you can send data across the Internet, which is less expensive than using a dedicated link, and mobile users can also use a VPN connection to connect to your network as they move from place to place. The only problem with this approach is that a remote site, as well as your main site, should use two ISPs to ensure that if one goes down, you still have a connection to the Internet. For a mobile user, this can be problematic if using an Internet service provided by the hotel. You can solve this problem by giving your users access to two different nationwide ISPs.

Another technology that can be used to provide an extra layer of redundancy, as well as high-speed access to storage devices, is the Storage Area Network (SAN). A SAN is a network that is separate from the LAN and contains only storage devices and servers that need to access those devices. Because the network bandwidth is not shared with LAN users, multiple servers can access the same storage. If one server fails, other servers can be configured to provide redundant access to the data. Also, the same RAID and other redundancy techniques used for storage devices that are directly attached to a server (such as the SCSI hardware and protocols) can be used on a SAN.

▶▶ The terms *RAID* and *UPS* are important in today's networks, as is the concept of load balancing and dual-redundant power supplies in large networks. You can find out more about RAID (Redundant Array Of Independent Disks) and UPSs (uninterruptible power supplies) by reading Chapter 5, "Protecting the Network: Preventative Maintenance Techniques." For more information about SANs, see Chapter 11.

The old saying "If it ain't broke, don't fix it" doesn't apply to networks. You should always be proactively looking for potential single points of failure and doing something to fix them. By building redundancy into the network design at the start, you'll save yourself a lot of grief in the future.

Chapter 5 can give you more suggestions about using clustering, backups, uninterruptible power supplies, and other techniques that can keep the network up and running.

Choosing a LAN Protocol

Today the de facto protocol of choice has to be TCP/IP. However, other protocols have their place in some vertical markets. In this book, we talk about NetWare. NetWare has been around so long that you might find you have no choice when designing an upgrade but to keep using IPX/SPX, depending on the applications your network uses. However, even NetWare has moved toward using TCP/IP as the underlying protocol. This is basically the case for version 5.x and 6.x of NetWare. Older

NetWare networks should upgrade, if possible, to one of these newer versions. If you will be connecting the network to the Internet, TCP/IP will be a necessity. Even if you don't expect to have an Internet connection, you'll find that choosing TCP/IP is a more practical choice today because most applications work with it and there is a large market of trained professionals who can be hired to manage a network built on TCP/IP. NetWare 6.x provides backward compatibility with IPX/SPX for the most part, but newer features such as the iPrint—which uses the Internet Printing Protocol—require TCP/IP.

Note

With Novell's purchase of Linux vendor SuSE and the introduction of the Novell Open Enterprise Server, which incorporates SuSE Linux, NetWare 6.5, and web services such as iPrint, it seems clear that Novell is moving away from NetWare and moving in the direction of providing network and Internet services.

In addition to transport protocols such as TCP/IP and IPX/SPX, you must consider application protocols that can be used on the network. For example, to simplify administering configuration information for a large number of computers, you might want to use the Dynamic Host Configuration Protocol (DHCP), which is discussed in Chapter 28, "BOOTP and Dynamic Host Configuration Protocol (DHCP)." If you want to provide a central name resolution service, you might choose the Domain Name Service (DNS), which is covered in Chapter 29, "Network Name Resolution." If you are going to operate a Windows network that has pre–Windows 2000/XP clients, you might need to use the Windows Internet Naming Service (WINS) for backward compatibility.

So when thinking about a network protocol, remember that it's not just one protocol you need to worry about. After you've decided which protocols are necessary, research the security implications of each.

It's Virtually Universal: TCP/IP

For all practical purposes, the standard LAN protocol today is TCP/IP. This is partly due to the rapid growth of the Internet, and the necessity of most businesses of having a Web presence, as well as the large number of vendors that have adopted this protocol suite. If your LAN is still using an older proprietary network protocol, you should seriously consider what it would take to upgrade to TCP/IP. Currently, TCP/IP version 4 is the most widely used protocol. In the future you can expect that the next version (IPv6) will start to find its way from the core of the Internet out to the edge, where your network resides. While technologies such as Network Address Translation (NAT) are widely employed to remedy the problem associated with the limited address space provided by IPv4, IPv6 will enable a much larger address space. Combine that with Network Address Translation, and the long-term bets are going to be on IPv6, or possibly some of the features that are part of IPv6. In addition to giving you a larger address space, IPv6 includes other important features. Those that will affect your network the most are security mechanisms, which will only become more important as Internet commerce continues to grow.

▶▶ For a detailed introduction to TCP/IP, see Chapter 24, "Overview of the TCP/IP Protocol Suite"; Chapter 25, "Basic TCP/IP Services and Applications"; and Chapter 27, "Troubleshooting Tools for TCP/IP Networks."

There is one very important reason you should consider TCP/IP as a LAN protocol: There are more trained professionals knowledgeable in TCP/IP than any other LAN protocol at this time. It is interesting to note that in Windows NT 3.51, the default network protocol was Microsoft's implementation of IPX/SPX (NWLink). In Windows NT 4.0 (and successive operating systems, from Windows 2000, XP, and Server 2003), the default network protocol is TCP/IP.

If your network is composed of several operating systems, from Windows to NetWare to Unix and Linux, then the bottom line is that TCP/IP is the lowest common denominator that will allow the

easiest connectivity and interaction between all of these. Even Microsoft's now-legacy NetBIOS/NetBEUI protocols have been adapted to run over TCP/IP.

Novell's NetWare Version 6.5

NetWare was perhaps the first attempt at seriously providing a LAN protocol that was easy to use. The basic file and print services offered by early versions of NetWare were much better than other solutions available at that time. After it became established in the business community, NetWare became the network solution of choice in many business environments that used the PC. Microsoft countered this success with its LANManager products, which were also marketed by other vendors in their own way, such as the Pathworks solution from Digital Equipment Corporation.

Today NetWare is a totally revamped solution to LAN connectivity. It provides many new features that are addressed to specifically make use of the Internet, and allow mobile users to connect to their home networks, as well as to enable NetWare users to make connections to outside networks. For example, the iPrint feature enables NetWare users to print to a printer on a remote network. For example, instead of sending a catalog that may be out of date in a month or so, you can use iPrint to periodically send specific information relevant to each customer, by printing it directly to the customer's printer.

And NetWare's iFolder allows mobile users to synchronize data stored on remote computers (such as a laptop computer) with the data stored on the company's network. Microsoft and other vendors offer similar features. However, the point to remember is that if you already are a NetWare user, you don't have to throw out your existing investment and move to a Microsoft network, or even a Unix/Linux environment. NetWare has changed as the market has changed, and you might find it less expensive to upgrade to NetWare 6.5 than to migrate to another platform. The bottom line involves not just the cost of migrating to another operating system, but the costs involved with retraining your network administrative personnel in new technology.

Because NetWare 6.5 is so tightly integrated with the IP protocol, and also offers backward compatibility with IPX/SPX, admins for existing NetWare networks should consider upgrading to NetWare 6.5 as well as considering other options.

If you want to move to Linux, Novell makes it easy by incorporating an enhanced version of NetWare 6.5 and SuSE Linux into its Novell Open Enterprise Server. Open Enterprise Server supports both Linux and NetWare-specific software and features, enabling you to move to Linux gradually.

Other LAN/WAN Protocols

The distinction between LAN and WAN (wide area networking) protocols is beginning to blur. Ethernet was once considered to be a LAN protocol. As time has passed, other technologies, such as Token-Ring, have become minor players in the LAN world. Yet the opposite is true of Ethernet. It has grown from a modest specification endorsed by Intel, DEC, and other vendors, such that it now can be considered a WAN protocol. The capabilities introduced by current LAN technologies are beginning to erode the differences between a LAN and a MAN (metropolitan area network). When the fourth edition of this book was published, Gigabit Ethernet was starting to fall into the inexpensive range of network topologies. That trend has continued and now 10Gigabit Ethernet (10GbE) is frequently being used in enterprise data centers. Today you may be using 100BASE-T for connecting client computers to the network, and Gigabit Ethernet to connect network segments via the network backbone. In some cases your network might even be exclusively based on 10GbE.

What does this mean to a network administrator today? With 10Gigabit Ethernet, you can use TCP/IP not only to create a local area network backbone, but to extend that reach to a metropolitan area network. And because TCP/IP is so intertwined with Ethernet, you can achieve an end-to-end MAN link that uses TCP/IP over faster Ethernet connections. Instead of employing more expensive solutions, such as SONET, you can now connect branch offices in the same geographical area using just TCP/IP.

You may not have to worry about installing expensive equipment used by SONET and other typical MAN protocols. Still, for the long haul—for example, between different cities—other protocols such as ATM and Frame Relay will come into play.

▶▶ For more information about SONET, ATM, and Frame Relay, see Chapter 15, "Dedicated Connections."

Planning and Design Components

When it is time to create a plan, what should the product of this effort be? Depending on the scope of the project, the end result might be a simple short document with a step-by-step checklist for adding a few network devices to the network to segment traffic. As the scope grows larger, so do the *receivables* that should be prepared for upper management as part of the plan. Some of the things you might want to consider including are listed here:

- **Documentation**—What kind of documents will be required to implement the plan? This can be in the form of checklists for both simple and complex upgrades, sign-off sheets, informational documents provided to end users, and so on. Don't forget training documentation that will be needed in a major upgrade. Training documentation should be prepared for both administrators and the highly skilled end users (power users) of new technology. Of course, you should have a document that shows the physical and logical layout of the network that is being implemented or upgraded. This sort of document can be very useful when something goes wrong and you are trying to troubleshoot a problem. You might find, for example, that the physical network you've designed cannot handle the load that users and applications will place on the network at certain points.
- **Overall project plan**—Any large project must be implemented in an orderly manner to be sure that the goals set for the plan are met, or possibly adjusted if necessary. A mechanism for feedback should always be included because the best of planning can always overlook some important features or applications that the current network offers. Creating a project plan with a liberal timeline can be very helpful for keeping the project on track by setting milestones to be met. By making the schedule a liberal one, you automatically build in extra time to be used when things don't go quite as you expected they would. If everything works perfectly, you get gold stars from management for bringing a project in early! Experience has shown that any large network upgrade plan will not perfectly match the first plan you develop.
- **Policies and procedures**—As with any technology, you should plan to develop documents that detail policies and procedures to follow when the new network begins operating. Policies dictate how the network is to be used. For example, you might not allow employees to use email for personal use or the Web browser to view pages not related to your business. Procedures are detailed instructions on how to perform certain actions. With new technology, both policy and procedure should be considered important factors.

Document Everything

Documentation is everything. People have very short memories of things that appear to have only a limited lifetime, such as work projects. It is important that a good project contain several important documents, listed here, but not limited to these:

- **An executive overview**—You must have some overall plan to present to upper management that explains, without too many technical details, the reasons the upgrade (or new network) is needed, and what benefits the business will obtain from the upgrade. In this sort of document, less is more. *Bulleted* items make a better point than long, prose-filled paragraphs. Point out the need for the network or the upgrade, and be sure to list the benefits for each point you make. If a benefit can be measured in dollars, be sure to include that information. You can include here the feedback you've obtained from the user community to show management why a change is necessary.

- **A technical project plan**—This is a difficult document to create. After you've identified the parts of the network to upgrade, you need to create lists of steps detailing the replacement of old equipment with the new, with little disruption to the user community. If you are building a network from scratch, or planning a major upgrade in which most of the existing equipment will be replaced, this kind of document works best when done in sections. A three-ring binder can be used, and individual sections can be assigned to technologically proficient team members for the initial writing of, and any possible updates to, sections of this document. In a larger network, it is more likely that you will have separate teams of network personnel implementing the project plan. If this is your case, create an overall plan, similar to the executive overview, and then create individual plans for each team to use for implementing their goals.

Note

Goals! If you include goals in your project plan (and you should), you can identify certain accomplishments that will be attained during the implementation of the project. These goals can be used to measure the performance of the plan, and can be used to adjust the schedule you have set for the project plan. Feedback from each project team can be used to modify the goals that you have set. It is rare that a project plan succeeds without some modifications. Plan for this, by reviewing each step in the process and creating alternative documents that can address each problem as it arises.

- **Detailed checklists**—For each task that must be performed, a detailed checklist can help ensure that an important step is not left out. This is a simple process, but it's a lot easier to get it right the first time if you use a checklist. However, creating a perfect checklist means that you've anticipated each and every possible situation that can occur. In large networks this is not always an easy task, because many applications tend to be user-centric. Be prepared to modify these checklists. As with disaster recovery plans, you should be sure to pass these checklists by lower-level administrative personnel, and provide some mechanism for testing them. Use the feedback you get to adjust your checklists as necessary.
- **Risk matrix**—Identify potential risks early in the project, as well as mitigation steps that may help avoid these risks, and a description of the impact to the project that will result if the issue does occur. Impact can include items such as timeline slip, features or benefits that will need to be dropped, additional equipment or budget needed to overcome an obstacle, or even complete project failure.

Test, Test, and Then Test Some More

After you have developed a plan and the requisite documentation, don't assume that all of your assumptions and calculations are accurate. The only way to determine that the products or applications you will use in the upgraded network will function as expected is to perform extensive testing. Microsoft resource kits always point out that for larger networks you should create a testing laboratory and try to test different combinations of applications and operating-system configurations and determine whether the results match the expectations of your plan.

For example, directory services are an important issue for large networks. Creating the directory structure may seem at first to be a simple task. You might simply create objects that match up to your company's organizational chart. Yet, what kind of interaction needs to occur between different departments? How can you structure the directory to make the job of granting access to other directory objects an easy task? Just as structured programming techniques make it easier to manage changes in applications as they are modified over time, creating a directory structure for a network should be done in a similar manner. Another reason why a well-designed directory structure is important is that it is through the directory that you can delegate management responsibilities to different administrators, without having to grant an administrator carte blanche access to directory objects that do not fall within their responsibility.

It is a good idea to solicit representatives of your user community for testing scenarios. Remember that the users are the most important part of your network. You can spend all the money in the world to buy the latest technology, but it will give you little value in return unless the user can continue to work efficiently.

Creating Policies and Procedures for Network Usage

Policies, mentioned earlier, are statements about how something should or should not be used. Policy documents are important for several reasons. First, you can't very well discipline an employee for abusing a network resource if you haven't created a usage policy that prohibits the particular abuse. If you don't want your network users to spend their lunch hours shopping for bargains on `eBay.com`, you should spell this out in an acceptable usage policy.

Policies are important in the design phase of the network because they detail how some resources are to be used. Using the example from the preceding paragraph, if you select an Internet connection after calculating what you expect your bandwidth requirements to be, you might find your network underperforming as users begin to use the connection for nonbusiness needs. Another situation in which policies come into play—to the point of being a necessity—is when you use a firewall. In Chapter 45, you'll learn more about how important it is to first create a security policy and *then* implement that security policy using firewall technology. If you don't know what kind of network traffic you want to allow through the firewall, setting one up is going to be difficult. For example, most secure sites prohibit users from the Internet to use the standard telnet application to gain access to computers inside the local network from computers located elsewhere on the Internet. Yet you might have users who work from home.

▶▶ In addition to Chapter 45, use all the other chapters in Part VIII, "System and Network Security," of this book to learn more about network security. You'll find chapters on basic security measures, both in the local LAN and in a wide area network (WAN), as well as chapters on encryption and virtual private networks (VPNs).

You can still keep your no-incoming-telnet policy and provide your users with a remote access server that can authenticate dial-in users or by using VPN technology. By finding out what users need in advance, you can include the necessary technology up front in the network design and might not have to make exceptions to policies later.

Procedures help prevent mistakes from happening in the first place. They are proactive measures that assist technical and nontechnical people when it comes to performing functions on the network. For example, in your network design you might have a team trained to set up several hundred desktop computers and attach them to the network. Although plugging the network card into the wall socket is simple, configuring the desktop machine can be a little more difficult. You'll need to either configure the desktop machine with valid addressing configuration information or set it up to use Dynamic Host Configuration Protocol (DHCP). Even though you might be doing this on a lot of computers, it's very easy to make a mistake when performing repetitive tasks. By using a checklist for each computer, you can improve your odds of getting it right the first time. Don't wait until you've created the network and then start looking for fires to put out. Instead, create procedure documents for commonly performed tasks. This includes tasks involved in the initial setup of the network, as well as procedures for performing daily tasks after the network is up and running—backups, connecting network drives, and so on.

Tip

Remember that wireless clients on a secure network must be configured manually, even if you plan to use DHCP for IP addresses. Each client must be configured with the correct SSID and encryption standard for your SOHO or corporate wireless network, and you must also assign a unique computer name and a common network or domain name for computers in the same workgroup or domain. Make sure your checklist also includes wireless-specific information.

Providing Training for Technical Personnel

Technical users who will be responsible for helping manage the network should be trained in the procedures for which they will be responsible. Again, this means you should provide training for those who will help you set up the network as well as those who will manage it after it is functioning. Training classes can be conducted by in-house personnel already familiar with the technology, or by one of the many hundreds of consulting services that make their living doing just this sort of thing. When it comes to training, consider cross-training support personnel so that if one person is out for the day (or longer), you still have a technician who can assist with the problem. The alternative is to have more than one person trained for specific areas of responsibility, and thus pay more in overhead costs.

Remember that the technical staff who support the network are the persons your users must depend on when a problem occurs. Perhaps the most expensive thing that can happen in most networks is *downtime*. RAID technology and backups can be used to protect data, but if you have hundreds (or even thousands) of idle workers getting paid to sit around while someone is reading a technical manual trying to determine the cause of a network problem, you might want to get your resume in order. Up-front training is not inexpensive, but downtime can be far more expensive than training the technical staff in the first place.

You Can't Forget the Budget (or Can You?)

When planning a network or an upgrade to a network, it is always tempting to use the latest, greatest gizmos. Sometimes, however, you can accomplish the same thing using a much less expensive gizmo. For example, if you have a small home office, you don't need a $2,000–$3,000 router and a T1 line to connect to the Internet. A simple cable or DSL modem and the appropriate broadband service should suffice in most instances. Inexpensive cable/DSL routers can be used to allow several computers on a small network to use this single connection (although some providers discourage, or even disallow this—check the details on your contract!). There is some debate as to whether the NAT and other firewall technology built into cable/DSL routers can serve as an adequate firewall. There are other protective steps that SOHO networks can employ, such as combining a router with NAT technology with a more complex software-based firewall and frequently updated virus-protection programs.

Plan the budget liberally, but don't include items that really aren't necessary. When you present a list of items to upper management that shows them what the new network will do for the company, the benefits should always outweigh the costs you've come up with. Although this might not be such an issue in a growing company, it's better to manage your network project responsibly so that you will maintain a good rapport with management. When you find that something you have planned and implemented isn't working as you expected, and you need to make changes, management will probably be more responsive if you've been frugal with the initial expenses incurred in building the network.

The Physical Network

After you've decided on the network protocols and the services you need to offer on the network, identified potential bottlenecks, and evaluated the security problems associated with your network needs, you can then design the physical aspects of the network.

The preceding chapter discussed different physical network topologies. There are tools you can use, such as Microsoft Visio, to draw a physical network diagram. Tools such as these are more expensive than a simple paint or drawing program but make a much better presentation to management than hand-drawn network layouts. Whichever tool you decide to use to create the actual network drawings, just be sure that the drawings are clear, concise, and accurate. Looking back at your network

application requirements, bandwidth requirements, and the like, you can then start designing the physical network, deciding where to place important servers and redundant devices.

Planning Resources

Finally, keep in mind that technology changes rapidly in the computer and networking fields. Although hubs might have been sufficient a few years ago, today these are now legacy devices that have been replaced by switches that operate much faster and cost about the same as a hub used to cost. Although Bill Gates might have thought (way back when) that no one would ever need more than 640KB of memory, that prediction proved false almost as soon as it left his mouth. As we all know, change is the only constant thing in this universe. With technology, this is especially the case today.

If you are about to set yourself on a course of designing a network, become familiar with all the latest technologies, and don't depend solely on past experience. The best way to keep up with new technologies is to read about them. You can use books, such as this one, and resources on the World Wide Web, and you can also talk to knowledgeable consultants who are experts in their field.

Finally, Appendix C, "Internet Resources for Network Administrators," can point you to some interesting books and Web sites that contain helpful information. You'll find links in the appendix to sites that specialize in security, network protocols, and so on. You'll also find sites that maintain copies of Internet Request for Comments (RFC) documents, which spell out standards that are used on the Internet.